Amendments to the Specification

Please replace the first, third and fourth paragraphs on page 1 with the following replacement paragraphs, respectively, marked-up to show changes:

This application is related to and claims ~~priority to~~ the benefit of U.S. provisional application entitled AUTHENTICATING SOFTWARE LICENSES having serial number 60/243718, by Raymond HO and Edward FUNG, filed on October 30, 2000 and incorporated by reference herein.

Software in a computer system may be distributed in a number of ways. From the perspective of preventing unauthorized use, these distribution methods may be classified into three groups, namely,[[:]] unrestricted entitlement, restricted entitlement, and non-entitlement methods.

Unrestricted entitlement means that the software distributed with a computer system will run on any computer system for which it was designed, without any restrictions. Apart from the licensing and contractual agreement, there is nothing in the software to guard against unauthorized use. This method is not desirable for expensive software.

Please replace the first, third, and fourth complete paragraphs on page 2 with the following replacement paragraphs, respectively, marked-up to show changes:

Non-entitlement means that the software is disabled when distributed, and requires a separate authorization method to enable the software. This method is commonly adopted in computer systems where a

single generic distribution medium is used to distribute all of the software, and software components or packages within may be enabled or disabled according to license contract.

The problem of software piracy is acute with a particular class of computer systems[[:]] ,namely Internet Appliances. An Internet Appliance is generally a computer system that performs some predetermined functions while connected to the Internet. The Internet Appliances typically consist of computer hardware with embedded software. The hardware includes a storage medium and a network interface card.

Software embedded in an Internet Appliance tends to be compact. It is not uncommon to store the entire system software in a storage medium that has only a few megabytes of capacity. This type of storage medium is usually small and very portable (such as CompactFlash and SIM cards). Because of wide adaptation and portability of such media, digital content inside such mediums media can be illegally duplicated very easily.

Please replace the fourth paragraph on page 3 with the following replacement paragraph, marked-up to show changes:

According to an aspect of the present invention, there is provided a method and an apparatus for using an encrypted unique digital signature ("engraved signature") as a uniquely definable signature to control the use or execution of software in a computer system. The computer system has a Network Interface Card ("NIC") with a Media Access Control ("MAC") address. On start up, the engraved signature is retrieved from the

persistent storage medium of the computer system and the MAC address is retrieved from the NIC. The MAC address is unique according to industry standards and therefore uniquely identifies the NIC being used in the computer system. A computed encrypted signature is generated using the MAC address and compared with the retrieved engraved signature. Where the computed encrypted signature does not match the engraved retrieved signature, the execution of the software is halted.

Please replace the first paragraph on page 4 with the following replacement paragraph, marked-up to show changes:

According to a further aspect of the present invention, there is provided a method of storing an engraved signature into a persistent storage medium by initializing [[said]]the medium with a blank signature, preferably during the software reproduction process. The blank signature is a unique predefined pattern of binary code. During system startup, the software protection program checks to determine if the signature in [[said]]the medium is blank or not. If blank, the protection software computes an encrypted signature based on the MAC address of the NIC in the computer system. The computed encrypted signature is stored in the persistent storage medium as the engraved signature for future authentication. Preferably, this process of engraving the signature is done once at the premises of a manufacturer before the computer system is shipped to the user.

Please replace the fourth paragraph on page 5 with the following replacement paragraph, marked-up to show changes:

The engraved signature 26, which is a 128-bit binary code, is stored in the persistent storage medium 20 as a 32-byte hexadecimal character string where every byte (8 [[bit]] bits) of the engraved signature is represented by 2 hexadecimal characters. The initial digital code of the engraved signature 26 is blank. A blank signature 26 is a predefined code pattern, the value of which is arbitrarily defined, but which value should not be the same as a signature computed from a MAC address.

Please replace the fifth paragraph beginning on page 5 and continuing on page 6 with the following replacement paragraph, marked-up to show changes:

The MAC address 18 embedded in the NIC 16 is a unique hardware identifier specified by the NIC hardware manufacturer. MAC addresses on all NICs are unique as per industry standard. The MAC address 18 is a 48-bit binary code created and encoded by the NIC manufacturer and is readable by the software running in the computer system 10. [[A]] The MAC address 18 of the computer system 10 is used to generate a computed encrypted signature ~~is generated based on the MAC address 18 of the computer system 10~~. The A non-blank engraved signature 26 is an encrypted signature based on one authorized MAC address.

Please replace the first, second and third complete paragraphs on page 6 with the following replacement paragraphs, respectively, marked-up to show changes:

The signature authentication program 24 authenticates software by comparing the computed encrypted signature by comparing it with the engraved signature 26. The software 28 is authorized or authenticated where the computed encrypted signature matches the engraved signature

26. The program 24 is preferably executed during the system start-up so that unauthorized use of the software 28 is detected as soon as possible, but the program 24 may also be executed at any time when the computer system 10 is running.

The engraved signature 26 is fabricated using unique hardware identification of the MAC address 18 by means of encryption. ~~An encryption method is implemented using a~~ The publicly available algorithm called Block Cipher SQUARE encryption method is used to generate the engraved signature. ~~The algorithm used is adopted from~~ Details of this encryption method can be found in the [[a]] published research paper by Joan Daemen, Lars Knudsen, and Vincent Rijmen. entitled "The Block Cipher Square", Eli Biham, editor, Fast Software Encryption '97, volume 1267 of Lecture Notes in Computer Science, pages 149--165, Haifa, Israel, January 1997, Springer-Verlag.

The ~~algorithm~~ Block Cipher Square encryption method is a one-way encryption method where the encryption key used to perform encryption is different from [[a]] the key used to perform decryption. Only the encryption method is required and used in accordance with this invention. It will however be understood by those skilled in the art that other encryption methods may also be used without departing from the scope of this invention.

Please replace the fourth paragraph beginning on page 6 and continuing on page 7 with the following replacement paragraph, marked-up to show changes:

The encryption method encodes and decodes 128-bit binary

numbers. The encryption method is a 2-step process in which an encryption key is generated in a first step and is used by in the second step to create the encrypted data. The MAC address 18 is only a 48-bit code. The rest of the 80-bit code is arbitrarily assigned to complete the 128-bit code input required by the encryption method. The 80-bit code is hard coded into the software protection program.

Please replace the first and second complete paragraphs on page 7 with the following replacement paragraphs, respectively, marked-up to show changes:

Referring to Figure 2, there is shown a flowchart of the steps for generating an encrypted signature 26 for the computer system 10 of Figure 1. At step 200, the MAC address 18 is read then, at step 202, the 48-bit MAC address 18 is combined with the 80-bit code [[for]] to yield a unique hardware ID. An encryption key is created using the unique hardware ID by [[the]] a key generation ("KeyGen") logic component of the software protection program (step 204). The encrypted signature is then created ~~from the encryption of~~ by encrypting the unique hardware ID using the encryption key (step 206). ~~Thus, the~~ The encrypted signature is the computed encrypted signature used by the signature authentication program 24 for authentication purposes ~~to the signature authentication program 24~~, and [[is]] forms the engraved signature 26 when the encrypted signature is created [[for]] by the signature engraving program 22.

Referring to Figure 3, there is shown a flowchart of the steps to ~~authenticate~~ provide the computer system 10 [[for]] with a license [[to]] for the software 28 according to the software protection program of Figure 1. At step 298, the signature authentication program 24 is started ~~by the~~ upon

execution of the software 28. At step 300, the engraved signature 26 is read from the persistent storage medium 20 and stored in RAM 14 for use [[by]] during later steps. At step 302, the MAC address 18 is read from the Network Interface Card 16 and then, at step 304, the computed encrypted signature is generated by encrypting the MAC address 18. At step 306, the computed encrypted signature is compared to the engraved signature 26. If No, the computed encrypted signature does not match with the engraved signature 26, then the execution of the software 28 is halted (step 308). If Yes, the computed encrypted signature matches the engraved signature 26, then the execution of the software 28 continues (step 310).

Please replace the first and third paragraphs on page 8 with the following replacement paragraphs, respectively, marked-up to show changes:

Referring to Figure 4, there is shown a flowchart of the steps to set up the software protection program with the engraved signature 26 of Figure 1. At step 400, the MAC address 18 is read from the Network Interface Card 16 and, at step 402, ~~display~~ the MAC address 18 is displayed to a user. The user then contacts the licensor of the software 28, provides the MAC address 18, and obtains a signature there from (step 404). The licensor uses the MAC address 18 to generate the computed encrypted signature for the user. The computed encrypted signature from the licensor is then saved by the user and stored as the engraved signature 26 (step 406).

Referring to Figure 5, there is shown a flowchart of the steps to automatically set up the software protection program with the engraved signature 26 of Figure 1. At step 500, the signature authentication program

24 is started [[by]] upon the execution of the software 28. At step 502, the engraved signature 26 is read from the persistent storage medium 20 and stored in RAM 14 for use [[by]] during later steps. At step 504, the MAC address 18 is read from the Network Interface Card 16 and then, at step 508, the computed encrypted signature is generated by encrypting the MAC address 18. At step 510, the engraved signature 26 is compared to determine if it is a blank signature. If Yes, the engraved signature 26 ~~matches the~~ is a blank signature, then, at step 512, the signature engraving program 22 engraves or stores the computed encrypted signature in the persistent storage medium 20 as the engraved signature 26. [[The]] In this case, execution of the software 28 continues (step 514). At step 512, the software protection program may disable or erase the signature engraving program 22 after one engraving for greater security.

Please replace the first and third paragraphs on page 9 with the following replacement paragraphs, respectively, marked-up to show changes:

If at step 510, the engraved signature 26 does not match the blank signature, then, at step 516, the computed encrypted signature is compared to the engraved signature 26. If No, the computed encrypted signature does not match with the engraved signature 26, then the execution of the software 28 is halted (step 518). If Yes, the computed encrypted signature matches the engraved signature 26, then the execution of the software 28 continues (step 514).

The computed signature that is stored as the engraved signature may further be encrypted using another one-way encryption method. In this embodiment, the computed signature is encrypted using an encryption

key of said another the other one-way encryption method by, for example, the manufacturer of the computer system during system integration. The signature authentication program only needs a decrypting key to read the engraved signature. In this manner, greater security can be achieved as the encryption key of said another one-way encryption method is not otherwise on the computer system.